(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 422 628 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
02.01.2019 Patentblatt 2019/01

(51) Int Cl.:
H04L 9/08 *(2006.01)* ***H04L 9/32*** *(2006.01)*
H04L 9/00 *(2006.01)*

(21) Anmeldenummer: **17178641.1**

(22) Anmeldetag: **29.06.2017**

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME
Benannte Validierungsstaaten:
MA MD

(71) Anmelder: **Siemens Aktiengesellschaft**
80333 München (DE)

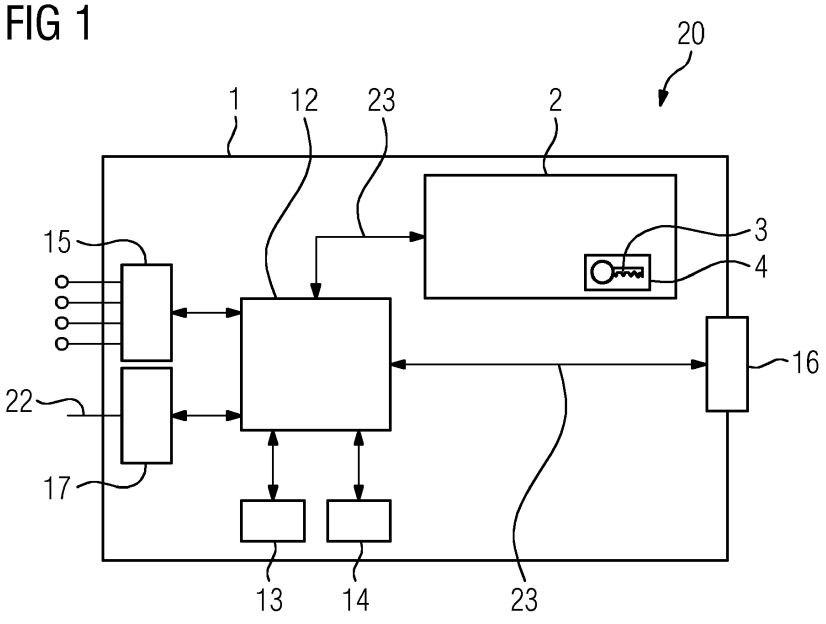
(72) Erfinder: **Falk, Rainer**
85586 Poing (DE)

(54) **VERFAHREN, SICHERHEITSEINRICHTUNG UND SICHERHEITSSYSTEM**

(57) Verfahren zum Erzeugen eines gerätespezifischen Gerätezertifikats (18, 18a - 18c) für ein Gerät (1, 1a - 1c), umfassend:
Koppeln (S1) einer Sicherheitseinrichtung (2) mit dem Gerät (1, 1a - 1c), wobei in der Sicherheitseinrichtung ein einmalig verwendbarer privater Signierschlüssel (3) gespeichert ist;
Speichern (S2) einer gerätespezifischen Identifizierungsinformation (21, 21a - 21c) in der Sicherheitseinrichtung (2);
Zugreifen (S3) auf den privaten Signierschlüssel (3) in der Sicherheitseinrichtung (2);
Erzeugen (S4) des gerätespezifischen Gerätezertifikats (18, 18a - 18c) in Abhängigkeit von der gespeicherten Identifizierungsinformation (21, 21a - 21c) in der Sicherheitseinrichtung (2), wobei das gerätespezifische Gerätezertifikat (18, 18a - 18c) mit dem privaten Signierschlüssel (3) signiert wird; und
Unterbinden (S5) eines weiteren Zugriffs auf den privaten Signierschlüssel (3).

Ferner werden eine Sicherheitseinrichtung zum Durchführen des Verfahrens sowie ein Sicherheitssystem mit der Sicherheitseinrichtung und dem Gerät vorgeschlagen. Mit dem beschriebenen Verfahren und der beschriebenen Sicherheitseinrichtung kann ein gerätespezifisches Gerätezertifikat (18, 18a - 18c) für ein Gerät (1, 1a - 1c) mit geringem Aufwand erzeugt werden, insbesondere ohne eine Public-Key-Infrastruktur einzusetzen.

FIG 1



EP 3 422 628 A1

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren und eine Sicherheitseinrichtung zum Erzeugen eines gerätespezifischen Gerätezertifikats für ein Gerät sowie ein Sicherheitssystem.

[0002] Um sicher in einem Kommunikationsnetzwerk mit einem Kommunikationspartner kommunizieren zu können, muss ein elektronisches Gerät, insbesondere ein Feldgerät, Steuergerät oder Internetder-Dinge-Gerät (IdD-Gerät) sich häufig bei dem Kommunikationspartner authentisieren. Durch die Authentisierung kann der Kommunikationspartner sicherstellen, dass eine Nachricht wirklich authentisch ist, also tatsächlich von dem angegebenen Gerät stammt. Das Gerät kann zum Beispiel anhand eines digital signierten Gerätezertifikats, welches gerätespezifische Information sowie einen öffentlichen Schlüssel des Geräts enthält, durch den Kommunikationspartner authentisiert werden. Das digitale Gerätezertifikat wird beispielsweise bei der Herstellung oder Inbetriebnahme des Geräts erstellt.

[0003] Zur Erstellung des Gerätezertifikats kann eine Public-Key-Infrastruktur (PKI) verwendet werden, welche anhand einer Zertifizierungsstelle, engl. "Certification Authority" (CA), eine Zertifikatsanfrage von dem Gerät erhält und ein digital signiertes Gerätezertifikat erzeugt. Das erstellte Gerätezertifikat muss dann über eine PKI-Schnittstelle auf das Gerät übertragen werden.

[0004] Weiterhin ist bekannt, ein Sicherheitsmodul mit einem sicherheitsmodulspezifischen Sicherheitsmodulzertifikat in ein Gerät einzubetten bzw. zu integrieren. Jedoch muss auch dabei zuerst ein Sicherheitsmodulzertifikat erstellt und über eine Schnittstelle an das Sicherheitsmodul übertragen werden. Dadurch kann zwar eine Authentisierung des Sicherheitsmoduls erfolgen, aber nicht des Geräts.

[0005] Vor diesem Hintergrund besteht eine Aufgabe der vorliegenden Erfindung darin, ein verbessertes Verfahren zum Erzeugen eines gerätespezifischen Gerätezertifikats für ein Gerät bereitzustellen. Weitere Aufgaben bestehen darin, eine verbesserte Sicherheitseinrichtung zum Erzeugen eines gerätespezifischen Gerätezertifikats für ein Gerät sowie ein verbessertes Sicherheitssystem zu schaffen.

[0006] Demgemäß wird ein Verfahren zum Erzeugen eines gerätespezifischen Gerätezertifikats für ein Gerät vorgeschlagen. Das Verfahren umfasst:

Koppeln einer Sicherheitseinrichtung mit dem Gerät, wobei in der Sicherheitseinrichtung ein einmalig verwendbarer privater Signierschlüssel gespeichert ist;
Speichern einer gerätespezifischen Identifizierungsinformation in der Sicherheitseinrichtung;
Zugreifen auf den privaten Signierschlüssel in der Sicherheitseinrichtung;
Erzeugen des gerätespezifischen Gerätezertifikats in Abhängigkeit von der gespeicherten Identifizierungsinformation in der Sicherheitseinrichtung, wobei das gerätespezifische Gerätezertifikat mit dem privaten Signierschlüssel signiert wird; und
Unterbinden eines weiteren Zugriffs auf den privaten Signierschlüssel.

[0007] Gemäß einer Ausführungsform wird ferner eine Sicherheitseinrichtung vorgeschlagen, welche eingerichtet ist, ein gerätespezifisches Gerätezertifikat für ein mit der Sicherheitseinrichtung gekoppeltes Gerät zu erzeugen. Die Sicherheitseinrichtung umfasst:

eine Schlüsselspeichereinrichtung zum Speichern eines einmalig verwendbareren privaten Signierschlüssels;
eine Identifizierungsinformationsspeichereinrichtung zum Speichern einer gerätespezifischen Identifizierungsinformation;
eine Zertifikaterzeugungseinrichtung zum Erzeugen des Gerätezertifikats in Abhängigkeit von der gespeicherten Identifizierungsinformation; und
eine Signatureinrichtung zum Signieren des Gerätezertifikats mit dem aus der Schlüsselspeichereinrichtung ausgelesenen privaten Signierschlüssel; wobei
die Sicherheitseinrichtung dazu eingerichtet ist, einen weiteren Zugriff auf den privaten Signierschlüssel zu unterbinden.

[0008] Gemäß einer weiteren Ausführungsform ist die Sicherheitseinrichtung dazu geeignet, das zuvor oder im Folgenden beschriebene Verfahren durchzuführen.

[0009] Die Sicherheitseinrichtung ist insbesondere ein physikalisches Hardware-Sicherheitsmodul, wie zum Beispiel ein Kryptocontroller, ein Secure Element (SE), ein Hardware-Vertrauensanker oder ein Trusted-Platform-Modul (TPM). Die Sicherheitseinrichtung kann separat von dem Gerät hergestellt werden, und zum Erstellen des Gerätezertifikats, zum Beispiel bei der Fertigung des Geräts, mit dem Gerät gekoppelt werden. Die Kopplung der Sicherheitseinrichtung mit dem Gerät kann über ein Kabel und/oder kabellos erfolgen. Die Sicherheitseinrichtung kann hierzu über eine Schnittstelle mit dem Gerät verbunden sein. Die Sicherheitseinrichtung kann auch in dem Gerät integriert sein. Das Gerät und die Sicherheitseinrichtung können derart miteinander gekoppelt sein, dass sie miteinander Daten austauschen können.

Die Sicherheitseinrichtung ist insbesondere von dem Gerät entfernbar.

[0010] Die Sicherheitseinrichtung vollzieht insbesondere die Funktionalität einer Zertifizierungsstelle. Sie kann verwendet werden, um für das Gerät ein gerätespezifisches, insbesondere einzigartiges digitales Gerätezertifikat zu erstellen. Bei dem Gerätezertifikat kann es sich um ein digitales Zertifikat nach dem kryptographischen Standard X.509 handeln. Zum Beispiel kann sich das Gerät mit dem Gerätezertifikat bei anderen Geräten in einem Netzwerk authentisieren, um mit diesen anderen Geräten Daten auszutauschen. Anhand des Gerätezertifikats kann das Gerät identifiziert werden. Unter Gerät sind insbesondere elektronische Geräte, zum Beispiel Feldgeräte, Steuergeräte und IdD-Geräte zu verstehen.

[0011] Nach dem Koppeln der Sicherheitseinrichtung mit dem Gerät kann die Sicherheitseinrichtung das Erstellen des Gerätezertifikats vornehmen. Hierbei kann die Sicherheitseinrichtung die gerätespezifische Identifizierungsinformation berücksichtigen, welche das Gerät insbesondere unverwechselbar charakterisiert. Zum Beispiel kann die gerätespezifische Identifizierungsinformation bei dem Erstellen des Gerätezertifikats in das Gerätezertifikat eincodiert werden. Durch die Berücksichtigung der gerätespezifischen Identifizierungsinformation, wie z.B. Hersteller, Gerätetyp, Hardware-Version, Firmware-Version und Seriennummer, beim Erstellen des Gerätezertifikats kann dem Gerätezertifikat seine Gerätespezifität verliehen werden. Verschiedene Geräte können dadurch unterschiedliche Gerätezertifikate erhalten. Insbesondere eignen sich die Gerätezertifikate daher zur Authentisierung der Geräte.

[0012] Das Erzeugen des Gerätezertifikats kann eine Vorbereitung eines Gerätezertifikatsentwurfs durch die Sicherheitseinrichtung umfassen. Der Gerätezertifikatsentwurf kann bereits alle Elemente eines fertig erstellten Gerätezertifikats enthalten, bei dem nur noch die digitale Signatur fehlt. Durch Signieren des Gerätezertifikatsentwurfs mit dem Signierschlüssel kann dann das Gerätezertifikat erstellt werden.

[0013] In einer Variante enthält der Gerätezertifikatsentwurfs eines oder mehrere Felder, z.B. z.B. Hersteller, Gerätetyp, Hardware-Version, Firmware-Version und Seriennummer, das oder die mit einem Wert zu belegen sind, bevor das Gerätezertifikat mit dem Signierschlüssel erstellbar ist.

[0014] Der Gerätezertifikatsentwurf kann in einer weiteren Variante Formatvorgaben (z.B. Länge, Zeichensatz) und zulässiger Wertebereiche für die zu belegenden Felder festlegen. Das Gerätezertifikat ist nur dann erstellbar, wenn alle auszufüllenden Felder mit einem Wert belegt sind, der den vorgegebenen Vorgaben gemäß dem Gerätezertifikatsentwurf entspricht.

[0015] In einer Weiteren Variante wird zumindest ein Feld, z.B. eine Geräteidentifizierungszeichenfolge (Gerätename), eine Geräteseriennummer, oder eine Zertifikatsseriennummer, mit einem zufällig bestimmten Wert automatisch belegt.

[0016] Der in der Sicherheitseinrichtung gespeicherte private Signierschlüssel ist insbesondere ein privater bzw. geheimer Signaturschlüssel, welcher nur ein einziges Mal verwendet werden kann. Insbesondere handelt es sich bei dem Signierschlüssel um einen kryptographischen Schlüssel. Er kann bereits bei der Herstellung der Sicherheitseinrichtung in der Sicherheitseinrichtung gespeichert werden.

[0017] Dadurch, dass der Signierschlüssel nur einmalig zum Signieren des Gerätezertifikats verwendbar ist, enthält die Sicherheitseinrichtung insbesondere die Funktionalität einer einmal-Zertifizierungsstelle, welche nur ein einziges Mal eine Gerätezertifikatsanfrage signieren kann und somit nur ein einziges Gerätezertifikat generieren kann. Eine einzige Sicherheitseinrichtung kann insbesondere nur ein einziges Gerätezertifikat ausstellen.

[0018] Die Sicherheitseinrichtung kann somit zum Beispiel auf einem beliebigen Gerät ein Gerätezertifikat erzeugen, ohne dass eine zentrale PKI benötigt wird. Insbesondere ist eine Anbindung des Geräts an eine PKI nicht erforderlich und das Gerät muss keine PKI-kompatible Schnittstelle aufweisen. Es ist auch nicht notwendig, während der Fertigung einen abgetrennten Sicherheitsbereich oder trainiertes Sicherheitspersonal zum Erstellen des Gerätezertifikats vorzusehen. Es kann also ein gerätespezifisches Gerätezertifikat mit geringen Aufwendungen erzeugt werden. Insbesondere ist es mit der Sicherheitseinrichtung auf einfache Weise möglich, ein sicheres Gerät mit einem Gerätezertifikat bereitzustellen.

[0019] Mit Hilfe der Sicherheitseinrichtung kann das Gerätezertifikat auch in einem Gerät, welches selbst keine Sicherheitsfunktionalität aufweist, erzeugt werden. Zum Erzeugen des gerätespezifischen Gerätezertifikats benötigt die Sicherheitseinrichtung lediglich die gerätespezifische Identifizierungsinformation. Somit kann ein beliebiges elektronisches Gerät mit einem Gerätezertifikat versehen werden. Mit dem Gerätezertifikat kann das Gerät zur sicheren Kommunikation mit anderen Geräten in einem Netzwerk authentisiert werden. Ferner können Geräte von unterschiedlichen Herstellern mit Sicherheitseinrichtungen bestückt werden, ohne dass die einzelnen Hersteller Sicherheitsanweisungen für das Erstellen von Gerätezertifikaten bekommen müssen und ohne dass die Geräte mit Sicherheitsmodulen ausstatten müssen.

[0020] Dadurch, dass der Signierschlüssel nur einmalig verwendbar ist, kann unterbunden werden, dass weitere Zertifikate mit dem Signierschlüssel signiert werden. Somit können insbesondere nach dem Erzeugen des einzigen gerätespezifischen Gerätezertifikats keine gefälschten Zertifikatsanfragen mit demselben Signierschlüssel signiert werden, wodurch keine gefälschten Gerätezertifikate erstellt werden können. Eine Authentizität des Zertifikats kann somit gewährleistet werden, wodurch die Sicherheit des mit dem Gerätezertifikat versehenen Geräts erhöht werden kann.

[0021] Mit der beschriebenen Sicherheitseinrichtung kann auf flexible Weise ein gerätespezifisches Gerätezertifikat

für ein bestimmtes Gerät erzeugt werden. Die Sicherheitseinrichtung muss insbesondere nicht während der Herstellung vorkonfiguriert zu werden. Stattdessen genügt zur Erzeugung des Gerätezertifikats die gerätespezifische Identifizierungsinformation.

[0022] Das Gerätezertifikat kann in dem Gerät und/oder in der Sicherheitseinrichtung gespeichert werden. Es kann ferner über ein Netzwerk an ein anderes Gerät (Kommunikationspartner) gesendet werden. Der Kommunikationspartner kann mit dem Gerätezertifikat die Authentizität des Geräts überprüfen und eine sichere Datenübertragung zwischen dem Gerät und dem Kommunikationspartner einrichten. Unter eine sichere Datenübertragung ist insbesondere eine kryptographisch verschlüsselte Datenübertragung zu verstehen, welche im Folgenden noch näher beschrieben wird.

[0023] Gemäß einer weiteren Ausführungsform umfasst das Unterbinden des weiteren Zugriffs auf den privaten Signierschlüssel ein Löschen des privaten Signierschlüssels, ein Überschreiben des privaten Signierschlüssels, ein Verändern des privaten Signierschlüssels und/oder ein Sperren eines Zugriffs auf die Schlüsselspeichereinrichtung, in der der private Signierschlüssel gespeichert ist. Das Löschen des Signierschlüssels kann hier sowohl ein logisches als auch ein physisches bzw. sicheres Löschen des Signierschlüssels sein.

[0024] Gemäß einer weiteren Ausführungsform sind in mehreren verschiedenen Sicherheitseinrichtungen gespeicherte Signierschlüssel identisch.

[0025] Insbesondere werden die mehreren Sicherheitseinrichtungen bei ihrer Herstellung alle mit identischen Signierschlüsseln versehen, sodass die mehreren resultierenden Sicherheitseinrichtungen komplett identisch sind. Insbesondere ist es nicht notwendig, die jeweilige Sicherheitseinrichtung im Hinblick auf das Gerät, mit welchem die Sicherheitseinrichtung bei der Fertigung gekoppelt werden soll, vorzukonfigurieren. Beispielsweise ist eine Information darüber, mit welchem Gerät die Sicherheitseinrichtung später gekoppelt werden soll, bei der Herstellung der Sicherheitseinrichtung nicht erforderlich. Dadurch kann eine Herstellung der Sicherheitseinrichtung unabhängig von einer Herstellung des Geräts erfolgen.

[0026] Es muss auch nicht darauf geachtet werden, welche Identifizierungsinformation ein bestimmtes Gerät während der Fertigung oder Programmierung erhalten wird. Somit bedarf die Herstellung der Sicherheitseinrichtung keine Vorkonfiguration der Sicherheitseinrichtung, wodurch ein vereinfachter Arbeitsablauf für das Programmieren des Geräts, insbesondere für das Erstellen des Gerätezertifikats für das Gerät ermöglicht wird.

[0027] Obwohl mehrere Sicherheitseinrichtungen einen gleichen Signierschlüssel aufweisen, kann für jedes Gerät mit Hilfe der gerätespezifischen Identifizierungsinformation ein unterschiedliches Gerätezertifikat generiert werden.

[0028] Gemäß einer weiteren Ausführungsform umfasst das Verfahren ferner ein Empfangen der gerätespezifischen Identifizierungsinformation von dem Gerät oder über eine Schnittstelle des Geräts in der Sicherheitseinrichtung oder ein Erzeugen der gerätespezifischen Identifizierungsinformation in der Sicherheitseinrichtung.

[0029] Die gerätespezifische Identifizierungsinformation kann bereits vor dem Koppeln der Sicherheitseinrichtung mit dem Gerät in dem Gerät gespeichert sein, und dann nach dem Koppeln mit der Sicherheitseinrichtung an diese übertragen werden.

[0030] Die gerätespezifische Identifizierungsinformation kann von außerhalb des Geräts über die Schnittstelle an die Sicherheitseinrichtung übertragen werden. Beispielsweise kann ein Benutzer die gerätespezifische Identifizierungsinformation über die Schnittstelle bereitstellen.

[0031] Ferner kann die gerätespezifische Identifizierungsinformation intern durch die Sicherheitseinrichtung erzeugt werden, insbesondere zufällig erzeugt werden. Bei hinreichend großen Wertbereichen für die gerätespezifische Identifizierungsinformation, zum Beispiel bei einer achtstelligen gerätespezifischen Identifizierungsinformation, ist die Wahrscheinlichkeit vernachlässigbar, dass zwei unterschiedliche Geräte identische zufällige gerätespezifische Identifizierungsinformation erzeugen. Eine vernachlässigbare Wahrscheinlichkeit ist insbesondere geringer als 10^{-5}. Es kann auch mit einer zufällig erzeugten gerätespezifischen Identifizierungsinformation ein eindeutiges gerätespezifisches Gerätezertifikat erzeugt werden.

[0032] Gemäß einer weiteren Ausführungsform umfasst das Verfahren ferner, in der Sicherheitseinrichtung:

Überprüfen, ob die gespeicherte Identifizierungsinformation in einem vorgegebenen Datenformat gespeichert ist; und

falls die gespeicherte Identifizierungsinformation in dem vorgegebenen Datenformat gespeichert ist, Erzeugen des gerätespezifischen Gerätezertifikats.

[0033] Insbesondere wird das Gerätezertifikat nur erzeugt, wenn bei der Überprüfung bestimmt wird, dass die gespeicherte gerätespezifische Identifizierungsinformation in dem vorgegebenen bzw. vorgespeicherte Datenformat vorliegt. Das vorgegebene Datenformat kann zum Beispiel einen zulässigen Wertebereich für die Identifizierungsinformation und/oder ein Format für die Identifizierungsinformation fordern und/oder bedingen. Das vorgegebene Datenformat kann bei einer Herstellung der Sicherheitseinrichtung definiert werden, oder durch einen Benutzer vorgegeben werden.

[0034] Gemäß einer weiteren Ausführungsform umfasst das Verfahren ferner, in der Sicherheitseinrichtung:

Empfangen einer Freischaltinformation;
Überprüfen, ob die Freischaltinformation mit einer vorgegebenen Freischaltinformation übereinstimmt; und
falls die Freischaltinformation mit der vorgegebenen Freischaltinformation übereinstimmt, Erzeugen des Gerätezertifikats.

[0035] Die Freischaltinformation ist beispielsweise ein Entsperrcode, ein Freischaltcode oder ein PIN. Die Freischaltinformation kann durch einen Benutzer oder von einem anderen Gerät über die Schnittstelle des Geräts an die Sicherheitseinrichtung übertragen werden. Insbesondere wird das Gerätezertifikat nur erzeugt, wenn bei der Überprüfung der Freischaltinformation erkannt wird, dass sie mit der vorgegebenen Freischaltinformation übereinstimmt. Die vorgegebene Freischaltinformation kann bei der Herstellung der Sicherheitseinrichtung in einer Speichereinrichtung der Sicherheitseinrichtung gespeichert werden.

[0036] Gemäß einer weiteren Ausführungsform umfasst das Verfahren ferner:

Erzeugen eines Geräteschlüsselpaars, welches einen öffentlichen und einen privaten Geräteschlüssel umfasst;
Speichern des privaten Geräteschlüssels in eine Schlüsselspeichereinrichtung des Geräts; und
Einbinden des öffentlichen Geräteschlüssels in das Gerätezertifikat beim Erzeugen des Gerätezertifikats.

[0037] Der private und der öffentliche Geräteschlüssel bilden insbesondere ein kryptographisches Geräteschlüsselpaar. Insbesondere erzeugt die Sicherheitseinrichtung das Schlüsselpaar. Der öffentliche Schlüssel kann beim Erzeugen des Gerätezertifikats derart in das Gerätezertifikat eingebunden bzw. eincodiert werden, dass ein Kommunikationspartner des Geräts den öffentlichen Schlüssel aus dem Gerätezertifikat erhalten kann, um mit Hilfe eines asymmetrischen kryptographischen Verfahrens mit dem Gerät zu kommunizieren. Insbesondere kann der Kommunikationspartner Daten, die für das Gerät bestimmt sind, mit dem öffentlichen Schlüssel verschlüsseln, sodass sie nur durch den in dem Gerät gespeicherten zugehörigen privaten Schlüssel entschlüsselt werden können und danach weiter nutzbar sind.

[0038] Gemäß einer weiteren Ausführungsform enthält die gerätespezifische Identifizierungsinformation zumindest eine Seriennummer des Geräts.

[0039] Gemäß einer weiteren Ausführungsform enthält das Gerätezertifikat die Identifizierungsinformation, eine Seriennummer des Gerätes, eine Information über eine Version des Geräts, eine Information über den Hersteller des Geräts, ein Zertifikatserstellungsdatum und/oder den privaten Geräteschlüssel. Die Information über die Version des Geräts kann insbesondere eine Version zum Hardware-Version des Gerätes und/oder eine Information zur Firmware-Version des Gerätes umfassen.

[0040] Gemäß einer weiteren Ausführungsform wird das Gerätezertifikat in einem vorgegebenen Zertifikatsformat erzeugt. Hierzu kann in der Sicherheitseinrichtung eine Zertifikatsvorlage enthalten bzw. gespeichert sein, die zumindest manche Felder des Gerätezertifikats vorgibt. Zum Beispiel kann die Reihenfolge der in dem Gerätezertifikat erhaltenen Informationen durch die Zertifikatsvorlage vorgesehen sein. Es kann auch ein Standard für das Zertifikat, beispielsweise der Standard X.509, durch die Zertifikatsvorlage vorgegeben sein.

[0041] Gemäß einer weiteren Ausführungsform wird ein Sicherheitssystem mit der beschriebenen Sicherheitseinrichtung und dem beschriebenen Gerät vorgeschlagen, wobei das Gerät eingerichtet ist, mit der Sicherheitseinrichtung gekoppelt zu werden. In Ausführungsformen sind die Sicherheitseinrichtung und das Gerät miteinander kommunikativ verbunden.

[0042] Die für das vorgeschlagene Verfahren beschriebenen Ausführungsformen und Merkmale gelten für die vorgeschlagene Sicherheitseinrichtung und für das vorgeschlagene Sicherheitssystem entsprechend.

[0043] Weitere mögliche Implementierungen des Verfahrens, der Sicherheitseinrichtung und des Sicherheitssystems umfassen auch nicht explizit genannte Kombinationen von zuvor oder im Folgenden bezüglich der Ausführungsbeispiele beschriebenen Merkmale oder Ausführungsformen. Dabei wird der Fachmann auch Einzelaspekte als Verbesserungen oder Ergänzungen zu der jeweiligen Grundform der Erfindung hinzufügen. Insbesondere ist eine Reihenfolge der beschriebenen Schritte modifizierbar.

[0044] Weitere vorteilhafte Ausgestaltungen und Aspekte der Erfindung sind Gegenstand der Unteransprüche sowie der im Folgenden beschriebenen Ausführungsbeispiele. Im Weiteren wird die Erfindung anhand von bevorzugten Ausführungsformen unter Bezugnahme auf die beigelegten Figuren näher erläutert.

Fig. 1 zeigt ein Sicherheitssystem gemäß einer ersten Ausführungsform;

Fig. 2 zeigt eine Sicherheitseinrichtung gemäß einer ersten Ausführungsform;

Fig. 3 zeigt ein Ablaufdiagramm für ein Verfahren zum Erzeugen eines gerätespezifischen Gerätezertifikats für ein Gerät gemäß einer ersten Ausführungsform;

Fig. 4 zeigt ein Ablaufdiagramm für ein Verfahren zum Erzeugen von gerätespezifischen Gerätezertifikaten für mehrere Geräte gemäß einer ersten Ausführungsform;

Fig. 5 zeigt ein Ablaufdiagramm für ein Verfahren zum Erzeugen eines gerätespezifischen Gerätezertifikats gemäß einer zweiten Ausführungsform; und

Fig. 6 zeigt eine sichere Kommunikation von Geräten in einem Netzwerk gemäß einer ersten Ausführungsform.

[0045] In den Figuren sind gleiche oder funktionsgleiche Elemente mit denselben Bezugszeichen versehen worden, sofern nichts anderes angegeben ist.

[0046] Die Fig. 1 zeigt ein Sicherheitssystem 20 gemäß einer ersten Ausführungsform. Das Sicherheitssystem 20 umfasst ein Gerät 1 mit einer eingebetteten Sicherheitseinrichtung 2, welche hier ein Hardware-Sicherheitsmodul (HSM) ist. Das Gerät 1 ist hier ein IdD-Feldgerät, das als ein Überwachungsfeldgerät in einer Produktionsstraße eingesetzt wird. Das IdD-Feldgerät 1 ist über eine Netzwerkschnittstelle 17 mit einem Netzwerk 22, hier einem Feldbus, verbunden. Das Netzwerk 22 umfasst weitere, nicht dargestellte IdD-Geräte, die über das Netzwerk 22 Daten mit dem IdD-Feldgerät 1 austauschen. Diese weiteren IdD-Geräte sind Kommunikationspartner für das IdD-Feldgerät 1, im Folgenden auch nur Feldgerät 1.

[0047] Das Feldgerät 1 umfasst ferner eine Ein- und Ausgabe-Schnittstelle 15, einen Prozessor 12, zwei Gerätespeichereinrichtungen 13, 14 und eine Benutzerschnittstelle 16. Die einzelnen Elemente des Feldgeräts 1 sind über Verbindungen 23, hier ein internes Bussystem, miteinander verbunden. Die Benutzerschnittstelle 16 ist hier eine USB-Schnittstelle, über welche ein Benutzer Daten an das Feldgerät 1 übertragen kann und Daten von dem Feldgerät 1 auslesen kann. Insbesondere wird das Feldgerät 1 bei der Programmierung über die USB-Schnittstelle 16 konfiguriert. Der Benutzer stellt zum Beispiel dem HSM 2 über die USB-Schnittstelle 16 eine noch im Folgenden beschriebene gerätespezifische Identifizierungsinformation zur Verfügung.

[0048] Die Ein- und Ausgabe Schnittstelle 15 ist als eine Einheit zum Verbinden mit externen Sensoreinheiten (nicht dargestellt) ausgeführt, mit welcher das Feldgerät 1 einen Druck und eine Temperatur am Feldgerät 1 erfassen kann. Erfasste Druck- und Sensordaten können in den Gerätespeichereinrichtungen 13, 14 gespeichert werden. Weiterhin können Aktoren mit der Ein- und Ausgabe Schnittstelle 15 verbunden werden. Beispielsweise kann ein Ventil als Aktor vom Feldgerät 1 angesteuert werden, wenn der erfasste Druck oder die erfasste Temperatur einen jeweiligen vorgebbaren Schwellwert überschreiten.

[0049] Die Gerätespeichereinrichtung 13 ist als ein RAM-Speicher ausgeführt, und die Gerätespeichereinrichtung 14 ist als ein Flash-Speicher ausgeführt. Die in den Gerätespeichereinrichtungen 13, 14 gespeicherte Druck- und Temperaturdaten können mit Hilfe eines im Folgenden näher beschriebenen privaten kryptographischen Schlüssels durch die Sicherheitseinrichtung 2 verschlüsselt werden und somit über das Netzwerk 22 sicher an die anderen Geräte bzw. Kommunikationspartner übertragen werden.

[0050] Das HSM 2 wird anhand der Fig. 2, welche eine Sicherheitseinrichtung 2 gemäß einer ersten Ausführungsform zeigt, näher beschrieben. Das HSM 2 umfasst eine Schlüsselspeichereinrichtung 4, eine Identifizierungsinformationsspeichereinrichtung 5, eine Zertifikaterzeugungseinrichtung 6 und eine Schnittstelle 8, welche über einen internen Bus 9 miteinander verbunden sind. Fakultativ kann das Sicherheitselement 2 zusätzlich auch noch eine Zertifikatspeichereinrichtung 10 und eine Vorlagenspeichereinrichtung 11 aufweisen.

[0051] Die Schnittstelle 8 dient zur Kopplung des HSM 2 mit dem Feldgerät 1. Daten können zwischen dem HSM 2 und dem Feldgerät 1 über die (physikalische) Schnittstelle 8 ausgetauscht werden. Bei der Herstellung des HSM 2 wird in der Schlüsselspeichereinrichtung 4, welche eine sichere Speichereinrichtung ist, ein HSM-unspezifischer Signierschlüssel 3 gespeichert. Der Signierschlüssel 3 ist hierbei ein einmalig verwendbarer privater Signierschlüssel.

[0052] Die Identifizierungsinformationsspeichereinrichtung 5 dient dazu, die von dem Benutzer über die USB-Schnittstelle 16 bereitgestellte Identifizierungsinformation 21 zu speichern. Die Zertifikaterzeugungseinrichtung 6 kann ein gerätespezifisches Gerätezertifikat 18 erstellen und signieren. In der Vorlagenspeichereinrichtung 11 ist eine Vorlage 7 für das Gerätezertifikat 18 gespeichert, welche beim Erzeugen des Gerätezertifikats 18 durch die Zertifikaterzeugungseinrichtung 6 herangezogen wird. Die Vorlage 7 bestimmt ein Format des zu erzeugenden Gerätezertifikats. In der vorliegenden Ausführungsform gibt die Vorlage 7 zum Beispiel vor, dass das Gerätezertifikat 18 eine Seriennummer und ein Zertifikatserstellungsdatum enthalten soll. Das Gerätezertifikat 18 ist ein digitales Zertifikat nach dem kryptographischen Standard X.509.

[0053] In einer Variante verfügt das HSM 2 über einen integrierten Zeitgeber als Echtzeituhr (Real Time Clock), was in der Figur nicht dargestellt ist. In einer anderen Variante wird der Zertifikaterzeugungseinrichtung 6 des HSM 2 eine Zeitinformation über die Schnittstelle 8 bereitgestellt. Die Zeitinformation kann von dem Prozessor 12 des Feldgeräts 1 von einem Zeitgeberbaustein (nicht dargestellt) des Feldgeräts 1 abgefragt und dem HSM 2 bereitgestellt werden. In einer weiteren Variante erstellt ein Zeitsynchronisationsserver, der mit dem Feldgerät 1 über die Netzwerkschnittstelle verbunden ist, eine durch eine kryptographische Prüfsumme geschützte Zeitsynchronisationsinformation, die von dem

Feldgerät 1 empfangen und dem HSM 2 bereitgestellt wird.

[0054] Das erzeugte Gerätezertifikat 18 kann dann in der Zertifikatspeichereinrichtung 10 gespeichert werden, um zur Authentisierung des Feldgeräts 1 verwendet zu werden.

[0055] Die Funktionalität der einzelnen Elemente des HSM 2 wird anhand der Fig. 3 näher beschrieben. Die Fig. 3 zeigt hierbei ein Verfahren zum Erzeugen eines gerätespezifischen Gerätezertifikats für ein Gerät 1 gemäß einer ersten Ausführungsform. Das in der Fig. 3 dargestellte Verfahren kann insbesondere durch das HSM 2 der Fig. 1 oder 2 durchgeführt werden, um ein Gerätezertifikat 18 für das Feldgerät 1 der Fig. 1 zu erzeugen.

[0056] In einem Vorbereitungsschritt S0 werden das Feldgerät 1 und das HSM 2 separat bereitgestellt. In der Schlüsselspeichereinrichtung 4 des HSM 2 ist bereits der Signierschlüssel 3 sicher gespeichert.

[0057] In einem Schritt S1 werden das HSM 2 und das Feldgerät 1 miteinander gekoppelt. Das HSM 2 wird bei dem Koppeln in einem Gehäuse des Feldgeräts 1 integriert. Die Kopplung des HSM 2 und des Feldgeräts 1 führt dazu, dass diese über die Schnittstelle 8 kommunizieren können.

[0058] In einem Schritt S2 wird eine gerätespezifische Identifizierungsinformation 21 in dem HSM 2 gespeichert. Die gerätespezifische Identifizierungsinformation 21 ist hier eine Seriennummer des Feldgeräts 1. Die Seriennummer 1 ist eine eindeutige alphanumerische Bezeichnung, die zur Identifikation des Feldgeräts 1 verwendet werden kann und somit gerätespezifisch ist. Die Seriennummer 21 wird durch den Benutzer über die USB-Schnittstelle 16 von dem Feldgerät 1 erhalten und über das interne Bussystem 23 an das HSM 2 übertragen. In dem HSM 2 wird die Seriennummer 21 in der Identifizierungsinformationsspeichereinrichtung 5 gespeichert.

[0059] In einem Schritt S3 wird in dem HSM 2 auf den privaten Signierschlüssel 3 zugegriffen. Hierbei wird der Signierschlüssel 3 durch die Zertifikaterzeugungseinrichtung 6 aus der Schlüsselspeichereinrichtung 4 ausgelesen.

[0060] In einem Schritt S4 wird das gerätespezifische Gerätezertifikat durch die Zertifikaterzeugungseinrichtung 6 erzeugt. Zunächst erzeugt die Zertifikaterzeugungseinrichtung 6 eine Zertifikatsvorlage nach dem Standard X.509, die einem nicht signierten Gerätezertifikat entspricht. Die Zertifikaterzeugungseinrichtung 6 greift hierbei auf die Vorlage 7 zu, die in der Vorlagenspeichereinrichtung 11 gespeichert ist. Ferner berücksichtigt die Zertifikatserzeugungseinrichtung 6 die empfangene Seriennummer 18 und codiert diese in die Zertifikatsvorlage mit ein.

[0061] Die Zertifikatsvorlage wird daraufhin durch die Zertifikaterzeugungseinrichtung 6 mit dem im Schritt S3 zugegriffenen Signierschlüssel 3 signiert. Dadurch entsteht das Gerätezertifikat 18 in dem durch die Vorlage 7 vorgegebenen Format. Es enthält insbesondere die in dem Schritt S2 erhaltene Seriennummer 21, wodurch die Gerätespezifität des Gerätezertifikats 18 gewährleistet wird. Das Gerätezertifikat enthält zum Beispiel ferner das Zertifikatserstellungsdatum. Das erzeugte Gerätezertifikat 18 wird in der Zertifikatspeichereinrichtung 10 gespeichert.

[0062] In einem Schritt S5 wird ein weiterer Zugriff auf den privaten Signierschlüssel 3 unterbunden. Hierzu wird der Signierschlüssel 3 aus der Schlüsselspeichereinrichtung 4 gelöscht, wie in der Fig. 2 durch den gestrichelt durchgestrichenen Signierschlüssel 3 dargestellt wird. Dadurch können keine weiteren Gerätezertifikate 18 mehr erzeugt werden.

[0063] Indem die Schritte S1 bis S5 durch das HSM 2 in dem Feldgerät 1 durchgeführt werden, wird für das Feldgerät 1 das gerätespezifische Gerätezertifikat 18 erstellt. Dadurch wird dem Feldgerät 1 seine Sicherheitsfunktionen verliehen. Das Gerätezertifikat 18 kann zur Erstellung einer sicheren Kommunikation mit einem anderen Gerät aus dem Netzwerk 22 an das andere Gerät (Kommunikationspartner) gesendet werden. Der Kommunikationspartner authentisiert das Feldgerät 1 mit dem empfangenen Gerätezertifikat 18, wodurch die sichere Kommunikation ermöglicht wird.

[0064] Die Fig. 4 zeigt ein Verfahren zum Erzeugen von gerätespezifischen Gerätezertifikaten für mehrere Geräte gemäß einer ersten Ausführungsform. Die Schritte S0 und S5 aus der Fig. 3 werden hierbei an drei Sicherheitssystemen 20a, 20b und 20c parallel durchgeführt. In der Fig. 4 werden parallel zueinander gerätespezifische Gerätezertifikate für drei verschiedene Feldgeräte 1a, 1b und 1c erzeugt. Die Gerätezertifikate werden hier nicht zur gleichen Zeit erzeugt, und die drei Sicherheitssysteme 20a, 20b und 20c befinden sich auch nicht am gleichen physikalischen Ort. Die Erstellung der drei Gerätezertifikate erfolgt unabhängig voneinander. Die Feldgeräte 1a, 1b und 1c umfassen die gleichen Komponenten wie das Feldgerät 1 aus der Fig. 1.

[0065] In dem Vorbereitungsschritt S0 werden die drei Feldgeräte 1a, 1b und 1c bereitgestellt. Diese sind identische Feldgeräte, denen unterschiedliche Seriennummern zugewiesen werden. Die Seriennummer ist eine eindeutige alphanumerische Bezeichnung, die zur Identifikation des Feldgeräts 1a, 1b, 1c verwendet werden kann und somit gerätespezifisch ist. In dem Vorbereitungsschritt S0 werden ferner drei komplett identische HSM 2 bereitgestellt, welche jede denselben Signierschlüssel 3 umfassen.

[0066] In dem Schritt S1 werden die Feldgeräte 1a, 1b und 1c jeweils mit einem HSM 2 gekoppelt. Die Kopplung erfolgt wie bereits in Bezug auf die Fig. 3 beschrieben. Dadurch werden die Sicherheitssysteme 20a, 20b und 20c gebildet.

[0067] In dem Schritt S2 gibt der Benutzer die Seriennummer 21a, 21b und 21c über die USB-Schnittstelle 16 in das Feldgerät 1 ein, welches diese über das interne Bussystem 23 an das HSM 2 weiterleitet. Somit erhält in dem Schritt S2 jedes der HSM 2 eine Seriennummer 21a, 21b und 21c und speichert diese in nicht dargestellten Identifizierungsinformationsspeichereinrichtungen 5. In den Schritten S3 und S4 wird auf die jeweiligen Signierschlüssel 3 zugegriffen, und es werden, unter Berücksichtigung der jeweiligen Seriennummern 20a, 20b und 20c Gerätezertifikate 18a, 18b und 18c erzeugt, die die Seriennummern 20a, 20b und 20c enthalten und mit den Signierschlüsseln 3 signiert sind.

[0068] In dem Schritt S5 wird ein weiterer Zugriff auf die jeweiligen Signierschlüssel unterbunden, indem diese aus den jeweiligen, nicht dargestellten Schlüsselspeichereinrichtungen 4 der HSM 2 gelöscht werden. In der Fig. 4 sind die gelöschten Signierschlüssel 3 gestrichelt und durchgestrichen dargestellt.

[0069] Die Fig. 4 zeigt somit, wie anhand des Verfahrens aus der Fig. 3 mit mehreren identischen HSM 2 in mehreren Feldgeräten 1a, 1b und 1c unterschiedliche, gerätespezifische Gerätezertifikate 18a, 18b und 18c zur Authentisierung der Feldgeräte 1a, 1b und 1c erzeugt werden können. Insbesondere wird hierzu keine zentrale PKI benötigt.

[0070] Obwohl in der Fig. 4 Gerätezertifikate 18a, 18b und 18c für drei Feldgeräte 1a, 1b und 1c erstellt werden, können in einem entsprechenden Verfahren Gerätezertifikate für beliebig viele Feldgeräte mit nur einem Typ von Sicherheitseinrichtungen bzw. HSM 2 erzeugt werden.

[0071] Die Fig. 5 zeigt ein abgewandeltes Verfahren zum Erzeugen eines gerätespezifischen Gerätezertifikats gemäß einer zweiten Ausführungsform. Mit dem Verfahren gemäß der zweiten Ausführungsform wird das Gerätezertifikat 18 nur erstellt, wenn gewisse Voraussetzungen erfüllt sind, wodurch das Gerätezertifikat 18 mit erhöhter Sicherheit erstellt wird. Das HSM 2 aus der Fig. 2 kann das Verfahren aus der Fig. 5 durchführen. In dem Verfahren gemäß der zweiten Ausführungsform sind die Schritte S0, S1, S2, S3, S4 und S5 identisch mit den Schritten S0 bis S5 aus der ersten Ausführungsform gemäß der Fig. 3 und werden nicht nochmal beschrieben.

[0072] Zusätzlich zu den Schritten S0 bis S5 wird in dem Verfahren gemäß der zweiten Ausführungsform vorgeschlagen, dass das HSM 2 in einem Schritt S11 nach dem Koppeln der HSM 2 mit dem Feldgerät 1 gemäß den Schritten S0 und S1 eine Freischaltinformation, hier einen Entsperrcode, empfängt. Der Entsperrcode wird durch den Benutzer über die USB-Schnittstelle 16 an das Feldgerät 1 übertragen und dann über die Schnittstelle 8 an das HSM 2 übermittelt.

[0073] Der empfangene Entsperrcode wird in einem Schritt S12 mit einem vorgegebenen Entsperrcode (z.B. 1234) als vorgegebene Freischaltinformation verglichen. In einer Variante wird die Gültigkeit des empfangene Entsperrcodes anhand einer vorgegebenen Prüfinformation überprüft. Der vorgegebenen Entsperrcode bzw. die vorgegebene Prüfinformation wird bereits bei der Herstellung des HSM 2 in der Identifizierungsinformationsspeichereinrichtung 5, im Folgenden auch nur Speichereinrichtung 5, geschützt gespeichert. Falls der empfangene Entsperrcode mit dem vorgegebenen Entsperrcode übereinstimmt bzw. falls der empfangene Entsperrcode anhand der vorgegebenen Prüfinformation als gültig überprüfbar ist, geht das Verfahren zum Schritt S2 über. Ansonsten werden die Schritte S11 und S12 widerholt, bis ein Entsperrcode empfangen wird, der mit dem vorgegebenen Entsperrcode übereinstimmt.

[0074] In einem Schritt S21 überprüft das HSM 2 ferner, ob die in dem Schritt S2 gespeicherte Seriennummer zulässig ist. Hierzu wird das Format der gespeicherten Seriennummer mit einem vorgegebenen Datenformat, welches bei der Herstellung des HSM 2 in der Identifizierungsinformationsspeichereinrichtung 5 gespeichert wird, verglichen. Das vorgegebene Datenformat gibt zum Beispiel vor, dass die Seriennummer drei Buchstaben und sechs Ziffern enthalten muss. Falls die Datenformate übereinstimmen, wird in dem Schritt S21 bestimmt, dass das Datenformat der gespeicherten Seriennummer zulässig ist, und das Verfahren wird mit einem Schritt S23 weitergeführt. Falls die Datenformate nicht übereinstimmen, werden die Schritte S2 und S21 wiederholt. Das heißt, es wird erneut einer Seriennummer durch den Benutzer eingegeben (S2), und es wird erneut überprüft, ob diese das vorgegebene Datenformat aufweist (S21).

[0075] In einem Schritt S23 erzeugt das HSM 2 ein kryptographisches Geräteschlüsselpaar mit einem kryptographischen privaten und einem kryptographischen öffentlichen Geräteschlüssel. Der private Geräteschlüssel wird in einem Schritt S24 in der Speichereinrichtung 5 gespeichert. Der private Geräteschlüssel wird zum Entschlüsseln von mit dem öffentlichen Geräteschlüssel verschlüsselten Daten benutzt.

[0076] In einem Schritt S41 wird die Zertifikatsvorlage mit der Zertifikaterzeugungseinrichtung 6 erstellt. Zusätzlich zur empfangenen Seriennummer 21 erhält die Zertifikatsvorlage auch den öffentlichen Geräteschlüssel, der in dem Schritt S23 erzeugt wurde.

[0077] In einem Schritt S42 wird die Zertifikatsvorlage mit dem Signierschlüssel 3 durch die Zertifikaterzeugungseinrichtung 6 signiert, und somit wird das Gerätezertifikat 18 fertig erstellt. Das Gerätezertifikat 18 enthält zumindest die Seriennummer 21 und den öffentlichen Geräteschlüssel. Die Schritte S41 und S42 sind Teil der bereits beschriebenen Schritte S3 und S4.

[0078] In dem Schritt S5 wird, wie bereits oberhalb beschrieben, der Signierschlüssel 3 gelöscht. In einem Schritt S6 wird das in dem Schritt S4 erzeugte Gerätezertifikat in der Zertifikatspeichereinrichtung 10 gespeichert.

[0079] Das Verfahren gemäß der zweiten Ausführungsform wird mit dem Schritt S7 beendet. Das Feldgerät 1 kann das Gerätezertifikat 18 an die weiteren Feldgeräte bzw. Kommunikationspartner in dem Netzwerk bzw. Feldbus 22 aus der Fig. 1 übersenden, damit diese es anhand der Information in dem Gerätezertifikat 18, insbesondere anhand der Seriennummer 21 authentisieren können. Es kann eine sichere Kommunikation zwischen dem Feldgerät 1 und den weiteren Feldgeräten erfolgen, weil die weiteren Feldgeräte mit dem Gerätezertifikat 18 des Feldgeräts 1 den öffentlichen Geräteschlüssel erhalten. Eine sichere Kommunikation bezeichnet hier einen Austausch von kryptographisch geschützten Daten.

[0080] Diese sichere Kommunikation zwischen dem Feldgerät 1 und einem weiteren Gerät 25 in dem Netzwerk 22 ist in der Fig. 6 dargestellt. Das weitere Gerät 25 ist auch ein Feldgerät und ist hier der Kommunikationspartner des Feldgeräts 1. Der Kommunikationspartner 25 ist hier ein elektrischer Motor. Das Feldgerät 1 und der Kommunikations-

partner 25 sind über das Netzwerk 22 miteinander gekoppelt. Wenn das Feldgerät 1 zuerst mit dem Kommunikationspartner 25 gekoppelt wird, übersendet es sein mit Hilfe des HSM 2 erstelltes Gerätezertifikat 18 an den Kommunikationspartner 25. Der Kommunikationspartner 25 liest die in dem Gerätezertifikat 18 enthaltenen Informationen, also die Seriennummer 21, das Zertifikatserstellungsdatum, den öffentlichen Geräteschlüssel usw., aus und überprüft so die Gültigkeit des Gerätezertifikats 18. Zur Überprüfung der Gültigkeit wird zum Beispiel anhand des Zertifikatserstellungsdatums überprüft, ob das Gerätezertifikat 18 noch nicht zu alt ist bzw. bereits abgelaufen ist.

[0081] Falls der Kommunikationspartner 25 bestimmt, dass das Gerätezertifikat 18 ungültig ist, weil es zum Beispiel bereits abgelaufen ist, wird die sichere Kommunikation zwischen dem Feldgerät 1 und dem Kommunikationspartner 25 nicht eingerichtet.

[0082] Falls der Kommunikationspartner 25 bestimmt, dass das Gerätezertifikat 18 gültig ist, wird die sichere Kommunikation zwischen dem Feldgerät 1 und dem Kommunikationspartner 25 eingerichtet. Diese erfolgt über das bereits vorhandene Netzwerk 22. Der Kommunikationspartner 25 verwendet den in dem Gerätezertifikat 18 erhaltenen öffentlichen Geräteschlüssel, um Daten zu verschlüsseln. Die Daten sind zum Beispiel Daten über einen Motorzustand, die an das Feldgerät 1 zu übertragen sind. Die verschlüsselten Daten werden über das Netzwerk 22 an das Feldgerät 1 übertragen, welches anhand des gespeicherten privaten Geräteschlüssels die empfangenen Daten entschlüsselt. Die entschlüsselten Daten können dann durch das Feldgerät 1 weiterverwendet werden, zum Beispiel modifiziert werden oder über die USB-Schnittstelle 16 an den Benutzer ausgegeben werden.

[0083] Die in der Fig. 6 dargestellte sichere Kommunikation zwischen dem Feldgerät 1 und dem Kommunikationspartner 25 kann entsprechend zwischen dem Feldgerät 1 und weiteren Kommunikationspartnern stattfinden.

[0084] Obwohl die vorliegende Erfindung anhand von Ausführungsbeispielen beschrieben wurde, ist sie vielfältig modifizierbar. Beispielsweise können beliebige elektronische Geräte, zum Beispiel IO-link Geräte, anstelle des beschriebenen IdD-Feldgeräts 1 verwendet werden. Dieses elektronische Gerät kann zudem beliebig aufgebaut sein und kann beispielsweise zusätzliche Schnittstellen und/oder Sensorelemente umfassen. Die Identifizierungsinformation kann eine beliebige gerätespezifische Information sein und kann anstelle der Seriennummer zum Beispiel auch eine Beschreibung des Geräts sein. Die Identifizierungsinformation kann auch als Zufallszahl durch die Sicherheitseinrichtung 2 erzeugt werden. Statt den Signierschlüssel zu löschen kann auch der Zugriff auf den Signierschlüssel gesperrt werden. Das erzeugte Gerätezertifikat kann auch in der Gerätespeichereinrichtung 13 gespeichert werden statt in der Sicherheitseinrichtung 2. Die Reihenfolge der in Fig. 3 und 5 beschriebenen Verfahrensschritte ist modifizierbar, zum Beispiel kann das Löschen des Signierschlüssels vor dem Erzeugen des Gerätezertifikats erfolgen.

Bezugszeichenliste

[0085]

1	Gerät
2	Sicherheitseinrichtung
3	Signierschlüssel
4	Schlüsselspeichereinrichtung
5	Identifizierungsinformationsspeichereinrichtung
6	Zertifikaterzeugungseinrichtung
7	Vorlage
8	Schnittstelle
9	interner Bus
10	Zertifikatspeichereinrichtung
11	Vorlagenspeichereinrichtung
12	Prozessor
13, 14	Gerätespeichereinrichtung
15	Ein- und Ausgabe Schnittstelle
16	Benutzerschnittstelle
17	Netzwerkschnittstelle
18, 18a, 18b, 18c	gerätespezifisches Gerätezertifikat
20, 20a, 20b, 20c	Sicherheitssystem
21, 21a, 21b, 21c	gerätespezifische Identifizierungsinformation
22	Netzwerk
23	internes Bussystem
24	Identifizierungsinformation
25	Kommunikationspartner
S0	Bereitstellen des Geräts und der Sicherheitseinrichtung

S1	Koppeln der Sicherheitseinrichtung mit dem Gerät
S11	Empfangen der Freischaltinformation
S12	Überprüfen, ob die Freischaltinformation mit einer vorgegebenen Freischaltinformation übereinstimmt
S2	Speichern der gerätespezifischen Identifizierungsinformation in der Sicherheitseinrichtung
S21	Überprüfen, ob die gespeicherte Identifizierungsinformation in einem vorgegebenen Datenformat gespeichert ist
S23	Erzeugen eines Geräteschlüsselpaars
S24	Speichern des privaten Geräteschlüssels in eine Schlüsselspeichereinrichtung
S3	Zugreifen auf den privaten Signierschlüssel
S4	Erzeugen des gerätespezifischen Gerätezertifikats
S41	Einbinden des öffentlichen Geräteschlüssels in das Gerätezertifikat beim Erzeugen des Gerätezertifikats
S42	Signieren der Zertifikatsvorlage mit dem Signierschlüssel durch die Zertifikaterzeugungseinrichtung
S5	Unterbinden eines weiteren Zugriffs auf den privaten Signierschlüssel
S6	Speichern des Gerätezertifikats in der Zertifikatspeichereinrichtung
S7	Beenden des Verfahrens

Patentansprüche

1. Verfahren zum Erzeugen eines gerätespezifischen Gerätezertifikats (18, 18a - 18c) für ein Gerät (1, 1a - 1c), umfassend:

   Koppeln (S1) einer Sicherheitseinrichtung (2) mit dem Gerät (1, 1a - 1c), wobei in der Sicherheitseinrichtung ein einmalig verwendbarer privater Signierschlüssel (3) gespeichert ist;
   Speichern (S2) einer gerätespezifischen Identifizierungsinformation (21, 21a - 21c) in der Sicherheitseinrichtung (2);
   Zugreifen (S3) auf den privaten Signierschlüssel (3) in der Sicherheitseinrichtung (2);
   Erzeugen (S4) des gerätespezifischen Gerätezertifikats (18, 18a - 18c) in Abhängigkeit von der gespeicherten Identifizierungsinformation (21, 21a - 21c) in der Sicherheitseinrichtung (2), wobei das gerätespezifische Gerätezertifikat (18, 18a - 18c) mit dem privaten Signierschlüssel (3) signiert wird; und
   Unterbinden (S5) eines weiteren Zugriffs auf den privaten Signierschlüssel (3).

2. Verfahren nach Anspruch 1, wobei das Unterbinden (S5) des weiteren Zugriffs auf den privaten Signierschlüssel (3) ein Löschen des privaten Signierschlüssels (3), ein Überschreiben des privaten Signierschlüssels (3), ein Verändern des privaten Signierschlüssels (3) und/oder ein Sperren eines Zugriffs auf eine Schlüsselspeichereinrichtung (4), in dem der private Signierschlüssel (3) gespeichert ist, umfasst.

3. Verfahren nach Anspruch 1 oder 2, wobei in mehreren verschiedenen Sicherheitseinrichtungen (2) gespeicherte Signierschlüssel (3) identisch sind.

4. Verfahren nach einem der Ansprüche 1 bis 3, ferner umfassend:

   Empfangen (S20) der gerätespezifischen Identifizierungsinformation (21, 21a - 21c) von dem Gerät (1, 1a - 1c) oder über eine Schnittstelle des Geräts in der Sicherheitseinrichtung (2), oder
   Erzeugen der gerätespezifischen Identifizierungsinformation (21, 21a - 21c) in der Sicherheitseinrichtung (2).

5. Verfahren nach einem der Ansprüche 1 bis 4, ferner umfassend: in der Sicherheitseinrichtung (2),
   Überprüfen (S21), ob die gespeicherte Identifizierungsinformation (21, 21a - 21c) in einem vorgegebenen Datenformat gespeichert ist, und
   falls die gespeicherte Identifizierungsinformation (21, 21a

   - 21c) in dem vorgegebenen Datenformat gespeichert ist, Erzeugen (S4) des gerätespezifischen Gerätezertifikats (18, 18a - 18c).

6. Verfahren nach einem der Ansprüche 1 bis 5, welches ferner umfasst: in der Sicherheitseinrichtung (2),
   Empfangen (S11) einer Freischaltinformation;

Überprüfen (S12), ob die Freischaltinformation mit einer vorgegebenen Freischaltinformation übereinstimmt; und falls die Freischaltinformation mit der vorgegebenen Freischaltinformation übereinstimmt, Erzeugen (S4) des gerätespezifischen Gerätezertifikats (18, 18a - 18c).

7. Verfahren nach einem der Ansprüche 1 bis 6, ferner umfassend:

Erzeugen (S23) eines Geräteschlüsselpaars, welches einen öffentlichen und einen privaten Geräteschlüssel umfasst;
Speichern (S24) des privaten Geräteschlüssels in eine Schlüsselspeichereinrichtung (4) des Geräts (1, 1a - 1c); und
Einbinden (S41) des öffentlichen Geräteschlüssels in das Gerätezertifikat (18, 18a - 18c) beim Erzeugen (S4) des Gerätezertifikats (18, 18a - 18c).

8. Verfahren nach einem der Ansprüche 1 bis 7, wobei die gerätespezifische Identifizierungsinformation (21, 21a - 21c) eine Seriennummer des Geräts (1, 1a - 1c) enthält.

9. Verfahren nach einem der Ansprüche 1 bis 8, wobei das Gerätezertifikat (18, 18a - 18c) die Identifizierungsinformation (21, 21a - 21c), die Seriennummer des Gerätes (1, 1a - 1c), eine Information über den Hersteller des Geräts (1, 1a - 1c), eine Information über eine Version des Geräts (1, 1a - 1c), ein Zertifikatserstellungsdatum und/oder den privaten Geräteschlüssel enthält.

10. Verfahren nach einem der Ansprüche 1 bis 9, wobei das Gerätezertifikat (18, 18a - 18c) in einem vorgegebenen Zertifikatsformat erzeugt wird.

11. Sicherheitseinrichtung (2), welche eingerichtet ist, ein gerätespezifisches Gerätezertifikat (18, 18a - 18c) für ein mit der Sicherheitseinrichtung (2) gekoppelten Gerät (1, 1a - 1c) zu erzeugen, umfassend:

eine Schlüsselspeichereinrichtung (4) zum Speichern eines einmalig verwendbareren privaten Signierschlüssels (3);
eine Identifizierungsinformationsspeichereinrichtung (5) zum Speichern einer gerätespezifischen Identifizierungsinformation (21, 21a - 21c); und
eine Zertifikaterzeugungseinrichtung (6) zum Erzeugen des Gerätezertifikats (18, 18a - 18c) in Abhängigkeit von der gespeicherten Identifizierungsinformation (21, 21a - 21c) und zum Signieren des Gerätezertifikats (18, 18a - 18c) mit dem aus der Schlüsselspeichereinrichtung (4) ausgelesenen privaten Signierschlüssel (3); wobei die Sicherheitseinrichtung (2) dazu eingerichtet ist, einen weiteren Zugriff auf den privaten Signierschlüssel (3) zu unterbinden.

12. Sicherheitseinrichtung (2) nach Anspruch 11, welche dazu geeignet ist, das Verfahren nach einem der Ansprüche 1 bis 10 durchzuführen.

13. Sicherheitssystem mit der Sicherheitseinrichtung (2) nach Anspruch 11 oder 12 und einem Gerät, welches eingerichtet ist, mit der Sicherheitseinrichtung (2) gekoppelt zu werden.

FIG 1

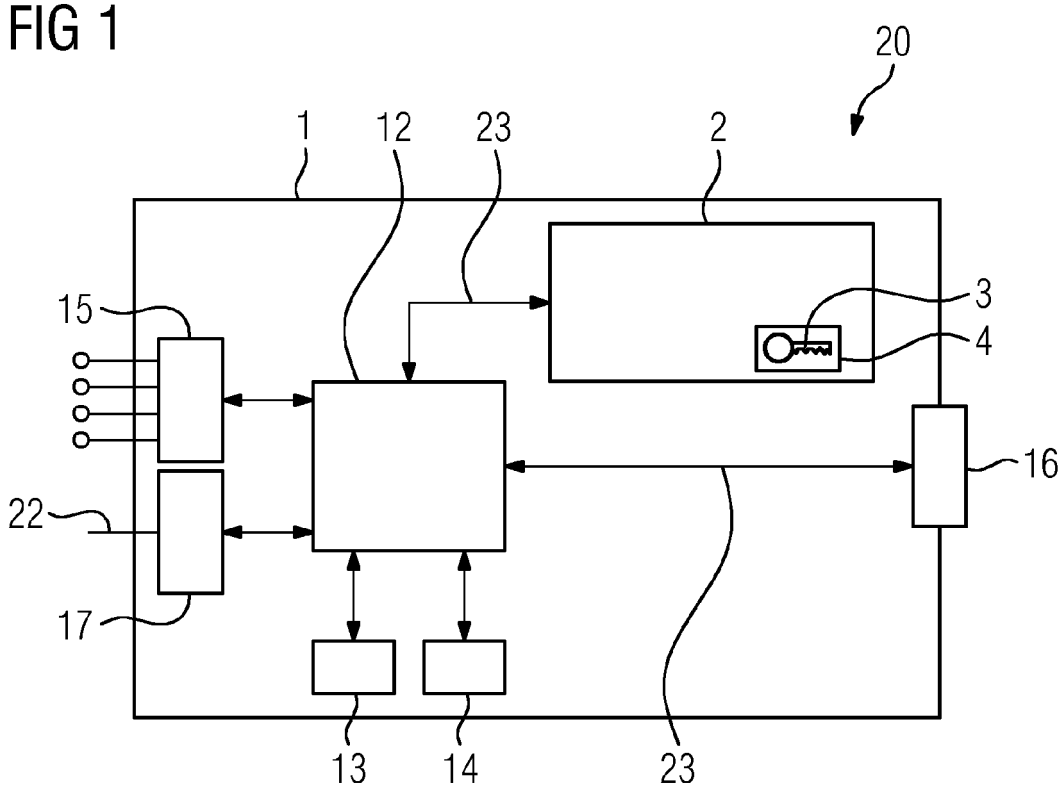


FIG 2

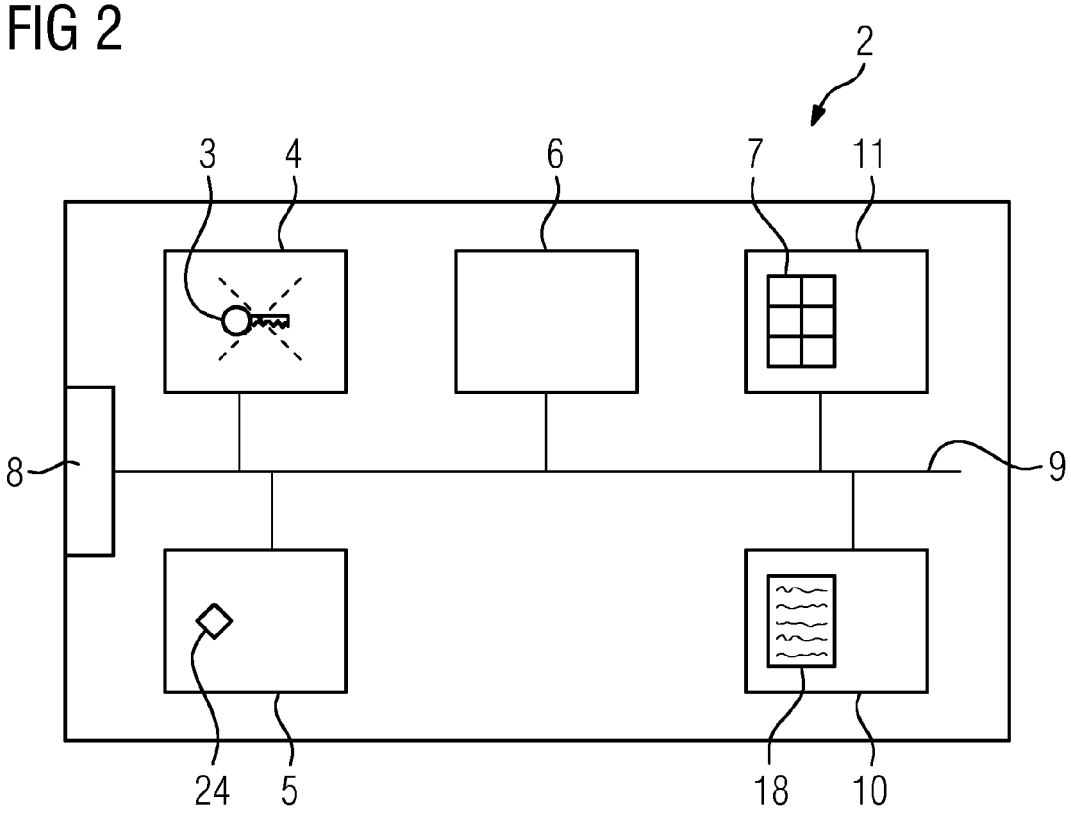


FIG 3

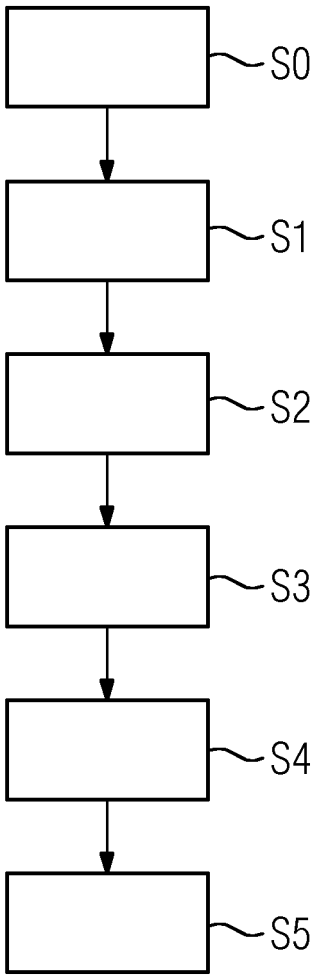


FIG 4

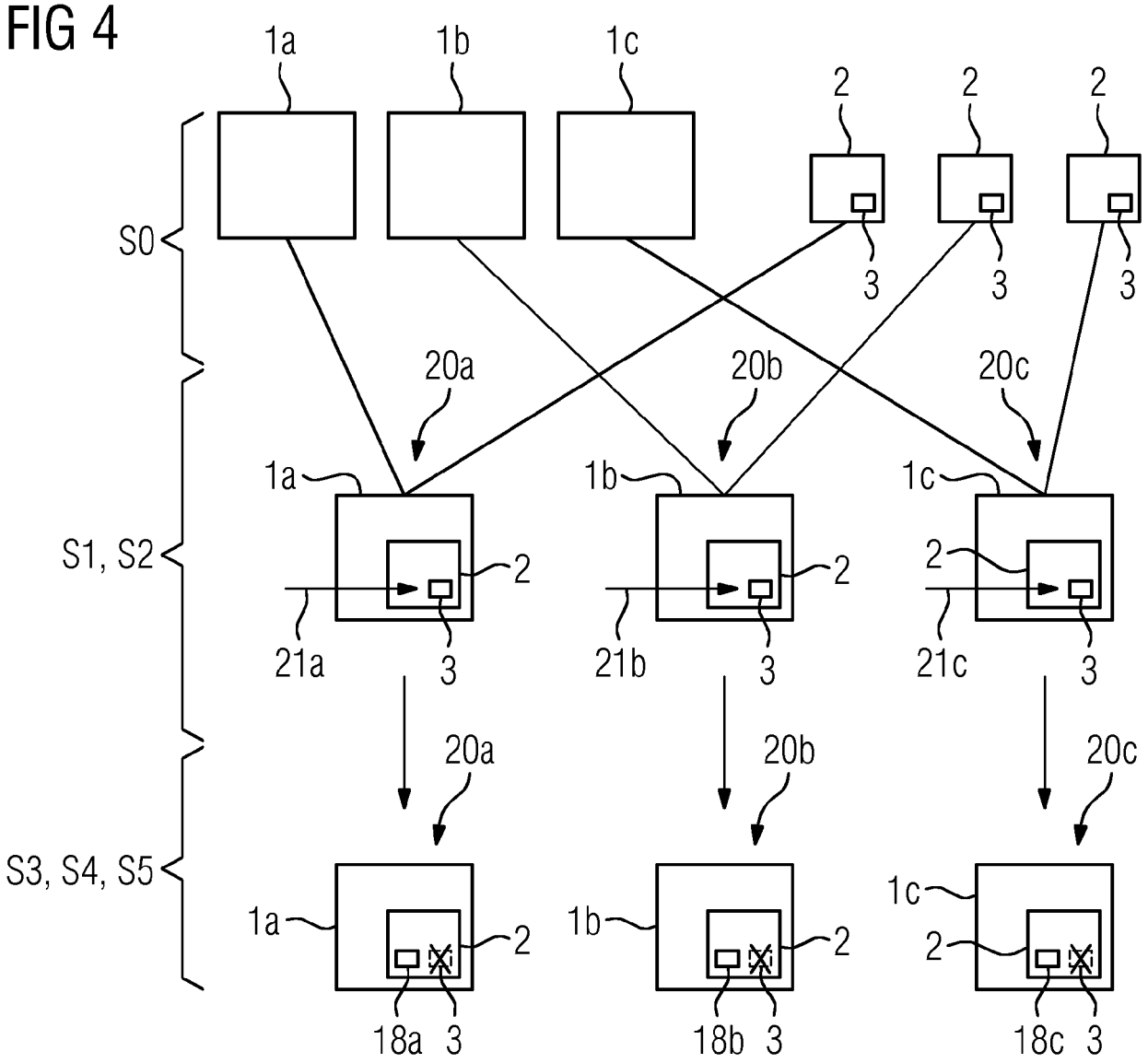

1a
1b
1c
2
2
2
S0
3
3
3
20a
20b
20c
1a
1b
1c
S1, S2
2
2
2
21a
3
21b
3
21c
3
20a
20b
20c
S3, S4, S5
1a
2
1b
2
1c
2
18a
3
18b
3
18c
3

FIG 5

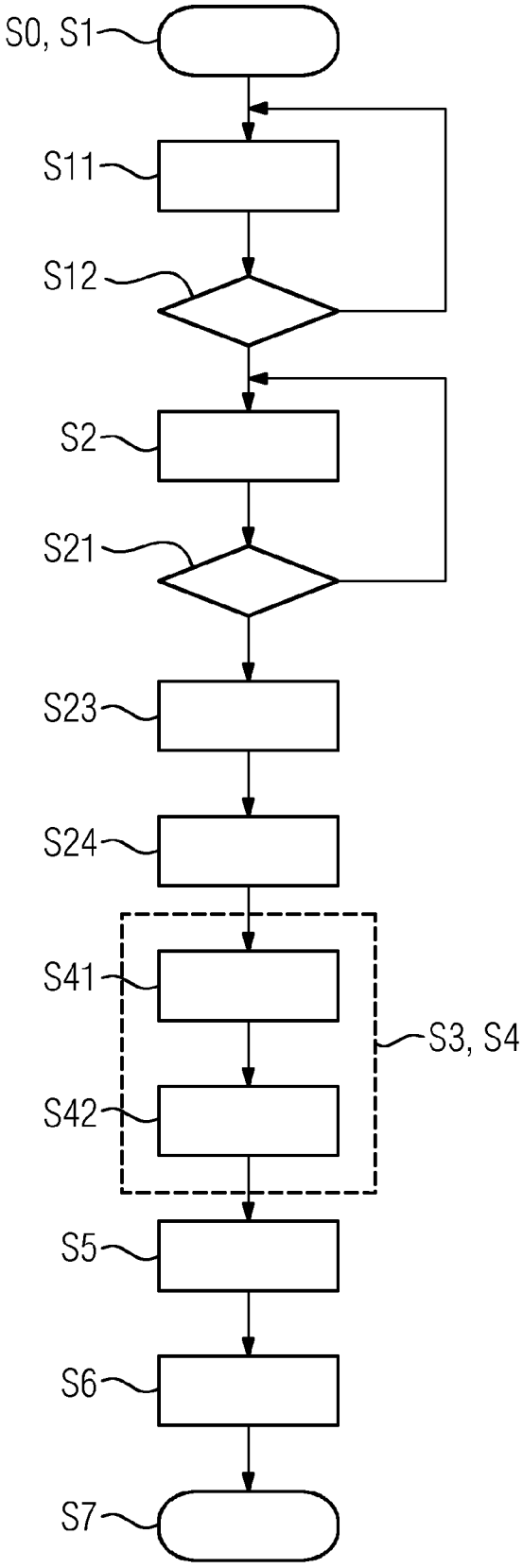
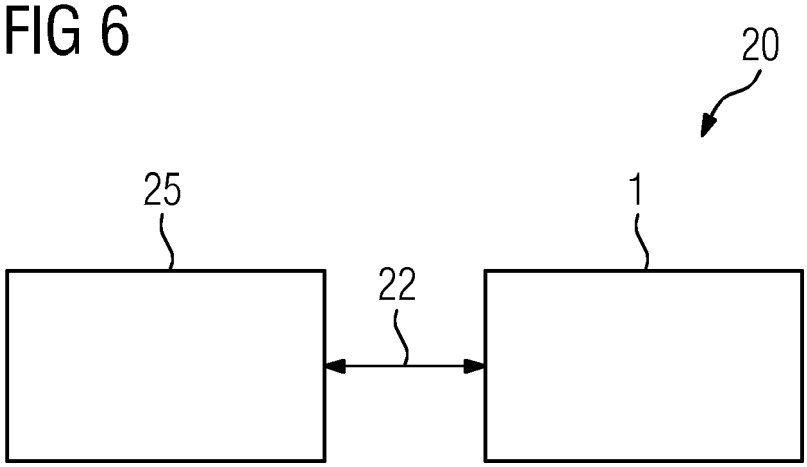


FIG 6



Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 17 17 8641

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
Y	DE 10 2013 205051 A1 (SIEMENS AG [DE]) 25. September 2014 (2014-09-25) * Absatz [0013] * * Absatz [0016] * * Absatz [0041] - Absatz [0056] * -----	1-13	INV. H04L9/08 H04L9/32 H04L9/00
Y	US 2006/020811 A1 (TAN TEIK G [SG]) 26. Januar 2006 (2006-01-26) * Absatz [0007] - Absatz [0012] * * Absatz [0056] - Absatz [0058] * -----	1-13	
A	DE 10 2014 102168 A1 (PHOENIX CONTACT GMBH & CO [DE]) 3. September 2015 (2015-09-03) * Absatz [0009] * * Absatz [0016] * * Absatz [0095] - Absatz [0107] * -----	1-13	

RECHERCHIERTE SACHGEBIETE (IPC)

H04L

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	5. Dezember 2017	Apostolescu, Radu

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 17 17 8641

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

05-12-2017

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102013205051 A1	25-09-2014	CN 105051627 A	11-11-2015
		DE 102013205051 A1	25-09-2014
		EP 2936259 A1	28-10-2015
		US 2016057134 A1	25-02-2016
		WO 2014146895 A1	25-09-2014
US 2006020811 A1	26-01-2006	AU 2005264830 A1	26-01-2006
		CA 2573101 A1	26-01-2006
		CN 1989731 A	27-06-2007
		EP 1771965 A1	11-04-2007
		JP 4879176 B2	22-02-2012
		JP 2008507892 A	13-03-2008
		KR 20070030284 A	15-03-2007
		US 2006020811 A1	26-01-2006
		WO 2006009517 A1	26-01-2006
DE 102014102168 A1	03-09-2015	CN 106031086 A	12-10-2016
		DE 102014102168 A1	03-09-2015
		EP 3108610 A1	28-12-2016
		US 2017054566 A1	23-02-2017
		WO 2015124726 A1	27-08-2015

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82